



Senate

General Assembly

File No. 190

January Session, 2005

Substitute Senate Bill No. 650

Senate, April 6, 2005

The Committee on General Law reported through SEN. COLAPIETRO of the 31st Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

AN ACT REQUIRING CONSUMER CREDIT BUREAUS TO OFFER SECURITY FREEZES.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1 Section 1. (NEW) (*Effective from passage*) As used in this section and
2 section 2 of this act:

3 (1) "Consumer" means consumer, as defined in section 36a-695 of
4 the general statutes;

5 (2) "Credit rating agency" means credit rating agency, as defined in
6 section 36a-695 of the general statutes;

7 (3) "Credit report" means credit report, as defined in section 36a-695
8 of the general statutes;

9 (4) "Creditor" means creditor, as defined in section 36a-695 of the
10 general statutes; and

11 (5) "Security freeze" means a notice placed in a consumer's credit
12 report, at the request of the consumer that prohibits the credit rating
13 agency from releasing the consumer's credit report or any information
14 from it without the express authorization of the consumer.

15 Sec. 2. (NEW) (*Effective from passage*) (a) Any consumer may submit
16 a written request, by certified mail or such other secure method as
17 authorized by a credit rating agency, to a credit rating agency to place
18 a security freeze on such consumer's credit report. Such credit rating
19 agency shall place a security freeze on a consumer's credit report not
20 later than five business days after receipt of such request from a
21 consumer if such request is accompanied by a case number issued by a
22 police department, and not later than fifteen days after receipt of such
23 request if such request is not accompanied by a case number issued by
24 a police department. Not later than ten business days after placing a
25 security freeze on a consumer's credit report, such credit rating agency
26 shall send a written confirmation of such security freeze to such
27 consumer that provides the consumer with a unique personal
28 identification number or password to be used by the consumer when
29 providing authorization for the release of such consumer's report to a
30 third party.

31 (b) In the event such consumer wishes to authorize the disclosure of
32 such consumer's credit report to a third party, or for a period of time,
33 while such security freeze is in effect, such consumer shall contact such
34 credit rating agency and provide: (1) Proper identification, (2) the
35 unique personal identification number or password described in
36 subsection (a) of this section, and (3) information regarding the third
37 party who is to receive the credit report.

38 (c) Any credit rating agency that receives a request from a consumer
39 to temporarily lift a security freeze on a credit report pursuant to
40 subsection (b) of this section shall lift such security freeze not later than
41 three business days after receipt of such request.

42 (d) Any credit rating agency may develop procedures involving the
43 use of telephone, facsimile, the Internet, or other electronic media to

44 receive and process such request from a consumer to temporarily lift a
45 security freeze pursuant to subsection (b) of this section.

46 (e) In the event that a third party requests access to a consumer's
47 credit report that has such a security freeze in place and such third
48 party request is made in connection with an application for credit or
49 any other use and such consumer has not authorized the disclosure of
50 such consumer's credit report to such third party, such third party may
51 deem such credit application as incomplete.

52 (f) Except for the temporary lifting of a security freeze as provided
53 in subsection (c) of this section, any security freeze authorized
54 pursuant to the provisions of this section shall remain in effect until
55 such time as such consumer requests such security freeze to be
56 removed. A credit rating agency shall remove such security freeze not
57 later than three business days after receipt of such request provided
58 such consumer provides proper identification to such credit rating
59 agency and the unique personal identification number or password
60 described in subsection (a) of this section at the time of such request
61 for removal of the security freeze.

62 (g) Any credit rating agency may decline to implement or may
63 rescind such security freeze request if such agency believes, in good
64 faith, that such request was made as part of a fraud that the consumer
65 participated in, or had knowledge of or can be demonstrated by
66 circumstantial evidence. In the event any such credit rating agency
67 declines to implement or rescinds a security freeze, such credit rating
68 agency shall promptly notify such consumer not later than five days
69 after such refusal.

70 (h) Nothing in this section shall be construed to prohibit disclosure
71 of a consumer's credit report by a credit rating agency to: (1) Any state
72 or local agency, law enforcement agency, court or private collection
73 agency acting pursuant to a court order, warrant or subpoena; (2) any
74 person or such person's subsidiary, affiliate, agent or assignee with
75 which the consumer has or, prior to assignment, had an account,
76 contract or debtor-creditor relationship for the purposes of reviewing

77 the account or collecting the financial obligation owing for the account,
78 contract or debt; (3) a state or municipal agency for the purposes of
79 collecting taxes, collecting child support or investigating fraud or any
80 other violation of the law; and (4) any person for the purposes of : (A)
81 Prescreening, as defined in 15 USC 1681 et seq., (B) administering a
82 credit file monitoring service to which the consumer has subscribed,
83 (C) providing the consumer with a copy of such consumer's credit
84 report upon the consumer's request, or (D) subdivision (2) or (3) of
85 subsection (f) of section 36a-699f of the general statutes.

86 Sec. 3. (NEW) (*Effective October 1, 2005*) As used in this section and
87 section 4 of this act:

88 (1) "Breach of the security of the system" means the unauthorized
89 acquisition of computerized data that contains personal information
90 from any person that maintains such personal information. "Breach of
91 the security of the system" does not include the acquisition, in good
92 faith, of personal information by any employee or agent of a person
93 that maintains such personal information for use by such employee or
94 agent in connection with such employee or agent's duties for such
95 person, provided such personal information is not used for a purpose
96 unrelated to the duties of such employee or agent and is not subject to
97 an unauthorized disclosure by such employee or agent; and

98 (2) "Personal information" means the first name or first initial and
99 the last name of any person in addition to any one, or more, of the
100 following nonencrypted pieces of information for such person: (A)
101 Social Security number; (B) driver's license number; or (C) any
102 financial account number, including a credit or debit card number
103 accompanied by the required security or access code for use of such
104 credit or debit card. "Personal information" does not include any
105 information available to the public from any record maintained by the
106 federal, state or any local government.

107 Sec. 4. (NEW) (*Effective October 1, 2005*) (a) Any person who, in the
108 ordinary course of such person's business, owns, maintains or licenses
109 computerized data that includes personal information shall notify any

110 resident of this state when such resident's nonencrypted personal
111 information has been or is reasonably believed to have been
112 improperly acquired by a third person due to a breach of the security
113 of the system. Such notification shall be made: (1) Either in writing, by
114 electronic mail or, if such breach of the security of the system affects
115 more than one hundred residents of this state, by publication on the
116 web site of such person and by public notification in or on
117 Connecticut-based newspapers, radio and television stations; and (2)
118 not later than fifteen days after such person's discovery of the breach
119 of the security of the system except that such notification may be
120 delayed upon the request of a law enforcement officer in furtherance of
121 a law enforcement investigation of such breach.

122 (b) Failure to provide any notice required by the provisions of
123 subsection (a) of this section shall constitute an unfair or deceptive
124 trade practice for purposes subsection (a) of section 42-110b of the
125 general statutes.

This act shall take effect as follows and shall amend the following sections:		
Section 1	<i>from passage</i>	New section
Sec. 2	<i>from passage</i>	New section
Sec. 3	<i>October 1, 2005</i>	New section
Sec. 4	<i>October 1, 2005</i>	New section

GL *Joint Favorable Subst.*

The following fiscal impact statement and bill analysis are prepared for the benefit of members of the General Assembly, solely for the purpose of information, summarization, and explanation, and do not represent the intent of the General Assembly or either House thereof for any purpose:

OFA Fiscal Note

State Impact:

Agency Affected	Fund-Effect	FY 06 \$	FY 07 \$
Consumer Protection, Dept.; Attorney General	Various - Revenue Gain	Potential Minimal	Potential Minimal

Municipal Impact: None

Explanation

The bill allows a consumer to freeze his credit report and requires businesses to inform the public if there has been a security breach involving their computerized personal information. This has no fiscal impact.

The bill also makes a violation of its provisions on security breaches an unfair trade practice. Under the Connecticut Unfair Trade Practices Act (CUTPA), the Department of Consumer Protection (DCP) and the Attorney General can impose CUTPA fines. In FY 04, \$18,789 was deposited in the General Fund as a result of such fines.

In the case of settlements, depending on the negotiation terms, funds are either deposited into the DCP's Consumer Protection Settlement Account or the General Fund. Funds deposited into the Consumer Protection Settlement Account are used only to enhance activities that further consumer protection. In FY 04, \$86,500 in CUTPA fines were deposited into the DCP Consumer Protection Settlement Account. Additionally, in FY 04, \$135,212 in CUTPA fines were deposited into the General Fund as a result of settlements negotiated by the Office of the Attorney General (OAG). The state agencies could accommodate the workload associated with enforcement of the bill without requiring additional resources. To the extent that the bill

increases the potential for future violations, the bill could result in a minimal revenue gain to the state.

OLR Bill Analysis

sSB 650

AN ACT REQUIRING CONSUMER CREDIT BUREAUS TO OFFER SECURITY FREEZES**SUMMARY:**

This bill (1) allows a consumer to freeze his credit report and (2) requires businesses to inform the public if there has been a security breach involving their computerized personal information.

The bill prohibits a credit rating agency from releasing a frozen credit report or any information in it without the consumer's express authorization. It requires an agency to freeze a report in five business days if a police case number accompanies a consumer's request. Otherwise, an agency has 15 days to freeze it. The bill creates a means by which a consumer can release his report, either permanently or temporarily. It allows an agency to deny a request to implement or remove a freeze if, in good faith, it believes the request is fraudulent. It authorizes a business to deem a credit application incomplete if it finds that the credit report is frozen. It exempts certain disclosures from the freeze.

The bill requires a business that has suffered a security breach to inform the public in writing or by e-mail. But if the breach involves more than 100 individuals, the bill requires a business to inform the public through Connecticut-based newspapers and television and radio stations.

EFFECTIVE DATE: Upon passage, except the provisions concerning security breaches take effect on October 1, 2005

SECURITY FREEZES

The bill allows a consumer to ask a credit rating agency to place a security freeze on his credit report. Consumer requests to freeze the report must be made in writing by certified mail or by another secure method authorized by the agency. The bill requires an agency to freeze

the report within (1) five business days if the request is accompanied by a police case number and (2) 15 days if the consumer did not submit a police case number. It requires an agency to keep the freeze in effect unless temporarily or permanently removed at the consumer's request. A "credit report" is a written or oral report, recommendation, or representation made by a credit rating agency relating to a consumer's credit worthiness, credit standing, or credit capacity, including information that sought to determine credit eligibility. A "consumer" is an individual seeking credit for personal, family, or household purposes.

The bill defines "security freeze" as a notice placed in a consumer's credit report, at his request, that prohibits an agency from releasing the report, or any information in it, without the consumer's express authorization.

Removing or Suspending a Freeze

The bill establishes a way for a consumer to remove the freeze or to temporarily release information in a credit report. It requires an agency to send the consumer a written confirmation including a unique personal identification number or password within 10 business days after freezing a report. The consumer can use the unique identifier to authorize the removal of the freeze or the report's release to a third party.

The bill requires an agency that has received a request to permanently or temporarily lift a freeze to do so by the third business day after receiving it. If a consumer wants to remove the freeze, he must provide (1) proper identification and (2) his unique identification number or password. If a consumer wants to disclose his information to a third party or for a period of time, he must provide (1) proper identification, (2) the unique identification number or password, and (3) information concerning the third party to receive the credit report. The bill authorizes agencies to develop procedures to receive and process the requests by telephone or through facsimile, the Internet, or other electronic means.

Denying a Request to Implement or Remove a Credit Freeze

The bill authorizes a credit agency to decline to implement or remove a credit freeze if it believes, in good faith, that the request was part of a

fraud that (1) the consumer participated in or knew about or (2) can be demonstrated by circumstantial evidence. In these cases, the bill requires an agency to promptly notify the consumer by the fifth day after the refusal.

Effect on Third-Party Requests

The bill authorizes a third party to deem a credit application incomplete if it requests access to a consumer's frozen credit report in conjunction with a credit application, or for another purpose, and the consumer has not authorized disclosure to the third party.

Exempted Disclosures

The bill allows agencies to disclose frozen credit reports to:

1. state or local agencies, law enforcement agencies, courts or private collection agencies acting under a court order, warrant, or subpoena;
2. any person, including a subsidiary, affiliate, agent, or assignee, with which a consumer has or had an account, contract, or debtor-creditor relationship for the purpose of reviewing the account or collecting a debt on it;
3. a state or municipal agency to (a) collect taxes or child support or (b) investigate fraud or any other violation;
4. anyone for (a) "prescreening" as defined by the federal law on credit rating agencies (see BACKGROUND), (b) administration of a credit file monitoring service to which a consumer subscribes, and (c) providing a consumer with a copy of his credit report at his request;
5. check or fraud prevention service companies that report on fraud for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar payment methods; and
6. demand deposit account information service companies that inform banks or other financial institutions reviewing a request for a demand deposit account about a potential consumer's account closures due to fraud, substantial overdrafts, automatic teller

machine abuse, or similar negative information.

DISCLOSING SECURITY BREACHES OF COMPUTERIZED DATA

The bill requires anyone who owns, maintains, or licenses computerized data containing non-encrypted personal information in the course of business to notify state residents whenever the information has been, or is reasonably believed to have been, acquired by a third party due to a breach of the security system. The bill defines “breach of the security system” as the unauthorized acquisition of computerized data that includes personal information. The bill provides that a breach does not include the acquisition, in good faith, of personal information by the business’s employee or agent in connection with his duties, if the information is not used for a purpose unrelated to his duties and is not disclosed without authorization.

“Personal information” is a person’s first name or initial and last name in addition to one or more of the following non-encrypted facts: (1) Social Security number; (2) driver’s license number; and (3) a financial account number, including a credit or debit card number with its security or access code. The bill excludes information available to the public from a federal, state, or local government.

The bill requires a business to notify the public of a security breach within 15 days after discovering it, but the notification may be delayed at the request of a law enforcement officer investigating the breach. If the breach affects up to 100 individuals, the notice may be sent in writing or by e-mail. If it affects more, the notice must be posted on the business’s website and published in Connecticut-based newspapers or broadcast on radio and television stations.

A violation of the bill’s provision on security breaches is an unfair trade practice.

BACKGROUND

Fair Credit Reporting Act

Federal law on credit rating agencies (15 USC 1681 *et seq.*) does not define “prescreening,” but it does prohibit states from adopting any requirements or prohibitions concerning prescreening reports for credit or insurance transactions not initiated by a consumer (15 USC §§ 1681t, 1681b(c), and 1681(e)).

Connecticut Unfair Trade Practices Act

The law prohibits businesses from engaging in unfair and deceptive acts or practices. CUTPA allows the DCP commissioner to issue regulations defining what constitutes an unfair trade practice, investigate complaints, issue cease and desist orders, order restitution in cases involving less than \$5,000, enter into consent agreements, ask the attorney general to seek injunctive relief, and accept voluntary statements of compliance. The act also allows individuals to sue. Courts may issue restraining orders; award actual and punitive damages, costs, and reasonable attorneys fees; and impose civil penalties of up to \$5,000 for willful violations and \$25,000 for violation of a restraining order.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute

Yea 15 Nay 0